Apple confirms iPhone, Mac affected by Meltdown-Spectre vulnerabilities

The iPhone maker has confirmed all Mac systems and devices running iOS are affected by the vulnerabilities, but also said there are currently no known exploits.

By Asha McLean | January 5, 2018 -- 03:01 GMT (19:01 PST) | Topic: Security - ZDNet

Apple has issued a statement regarding the Meltdown and Spectre vulnerabilities, confirming all Mac systems and iOS devices are affected, but saying there are no known exploits impacting customers at this time.

Apple, like Microsoft, has urged users to download software only from trusted sources, such as the App Store. The iPhone maker has already released mitigations in iOS 11.2, macOS 10.13.2, and tvOS 11.2 to help defend against Meltdown, and confirmed on Thursday the Apple Watch is not affected by Meltdown.

"In the coming days we plan to release mitigations in Safari to help defend against Spectre," the company said in a statement. "We continue to develop and test further

mitigations for these issues and will release them in upcoming updates of iOS, macOS, tvOS, and watchOS."

The researchers who discovered the vulnerabilities said that "almost every system," since 1995, including computers and phones, is affected by the bug. The researchers verified their findings on Intel chips dating back to 2011, and released their own proof-of-concept code to allow users to test their machines.

"An attacker might be able to steal any data on the system," said Daniel Gruss, a security researcher who discovered the Meltdown bug, in an email to ZDNet.

"Meltdown is not only limited to reading kernel memory but it is capable of reading the entire physical memory of the target machine," according to the paper accompanying the research.

The vulnerability affects operating systems and devices running on Intel processors developed in the past decade, including Windows, Macs, and Linux systems.

The Meltdown and Spectre issues take advantage of a modern CPU performance feature called speculative execution, which improves speed by operating on instructions may be used in future.

To increase performance, the CPU predicts which path of a branch is most likely to be taken, and will speculatively continue execution down that path even before the branch is completed. If the prediction was wrong, this speculative execution is rolled back in a way that is intended to be invisible to software.

According to Apple, the Meltdown and Spectre exploitation techniques abuse speculative execution to access privileged memory -- including that of the kernel -- from a less-privileged user process such as a malicious app running on a device.

While Linux can deal with the fundamental issue with Meltdown, Linux creator Linus Torvalds shared his displeasure on the situation to the Linux Kernel Mailing List.

"I think somebody inside of Intel needs to really take a long hard look at their CPU's, and actually admit that they have issues instead of writing PR blurbs that say that everything works as designed," he wrote.

"... and that really means that all these mitigation patches should be written with 'not all CPU's are crap' in mind.

"Or is Intel basically saying 'we are committed to selling you shit forever and ever, and never fixing anything?'

Because if that's the case, maybe we should start looking towards the ARM64 people more."

A Linux security expert told ZDNet that Google Project Zero informed Intel about the security problems in April, but neither Google nor Intel bothered to tell the operating system vendors until months later.

This resulted in Apple, Linux developers, and Microsoft to scramble to deliver patches to fundamental CPU security problems.

Microsoft has also warned users that its patches for Meltdown won't reach them if their third-party antivirus hasn't been updated to support this week's Windows security update.

original article:
http://www.zdnet.com/article/apple-confirms-iphone-mac-affected-by-meltdown-spectre-vulnerabilities/?loc=newsletter_large_thumb_featured&ftag=TRE-03-10aaa6b&bhid=23405847687286447375579737817622